UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/445,133	03/13/2000	AHMET MURSIT ESKICIOGLU	RCA88674	9526

24498 7590 12/26/2006

THOMSON LICENSING INC.
PATENT OPERATIONS
PO BOX 5312
PRINCETON, NJ 08543-5312

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	12/26/2006	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/445,133	ESKICIOGLU, AHMET MURSIT	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 10/16/06. The amendment filed on 10/16/06 have been entered and made of record. Therefore, presently pending claims are 1-20.

Response to Arguments

Applicant's arguments filed 10/16/06 have been fully considered.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., authenticating a source of a digitally signed encrypted message in response to receiving a digitally signed encrypted message, and decrypting the digitally signed encrypted message to obtain the descrambling key upon the authenticating (emphasis added)) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The applicant argued further that Kaplan is not understood to teach or suggest authenticating a guide provider by decrypting a digital signature using a public key of the guide provider, with the guide public key being stored in the device and decrypting the message using a private key of the smart card to obtain even information and the symmetric key, the smart card private key being stored within the smart card. In reference to the smart card, the new grounds of rejection using Vancelette discloses the smart card. However the limitation of authenticating

a guide provider (publisher), is disclosed by Kaplan (page 5 and page 2). The public key of the publisher that is provided in the certificate, and therefore stored in the device, is used to authenticate the digital signature of the publisher, wherein the publisher uses their private key to encrypt the digital signature.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Kaplan ("IBM Cryptolopes, Super Distribution and Digital Rights Management") in view of Renaud (6,021,491).

In reference to claim 1, Kaplan discloses the cryptolope system wherein the user device receives an electronic list of events (programs; Figure on page 3), at least one event having a digitally signed encrypted message associated therewith (page 3), said encrypted message comprising a descrambling key and event information including payment amount corresponding to said associated event (Terms and Conditions page 4); and receives in said device, in response to user selection of said event, said digitally signed encrypted message (page 3 and page 6). The user device receives the program after requesting in program as shown on the figure on page 3. The system of Kaplan further authenticates, in the user, the source, the producer, of the digitally

signed encrypted message in response to said digitally signed encrypted message (page 5 and page 7 Buying a Cryptolope part 2 and page 2 Cryptolope-a cryptographic envelope, paragraph 2); decrypting in said devices said digitally sired encrypted message to obtain said descrambling key upon said authenticating (page 7 Buying a Cryptolope part 5); receives, in said device, said selected event from the service provider (Publisher Content Creator paragraph), said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event (Figure on page 6); and descrambles, in said device, said selected event using said descrambling key (part 8 of Buying a Cryptolope page 7).

Although Kaplan discloses the authentication of the digital signature of the produces, the source, the system of Kaplan also discloses the authentication among participants. However Kaplan does not expressly disclose the authentication in the receiving device.

Renaud discloses a method, apparatus, and products are provided for verifying the authenticity of data within one or more data files (abstract). Renaud discloses the user receiving a signed file that it verifies the authenticity of the signed signature file (column 7 lines 48-62).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the contents of files as in Renaud using the digital signature and system of Kaplan. One of ordinary skill in the art would have been motivated to do this because digital signature verification provides a relatively high level of confidence in the authenticity of the source of the received data (Renaud column 2 lines 1-10).

Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan in view of Renaud in view of the book by Schneier (Applied Crptography).

In reference to claim 18, Kaplan discloses the cryptolope system wherein the user device receives an electronic list of events (programs; Figure on page 3), at least one event having a digitally signed encrypted message associated therewith (page 3), said encrypted message comprising a descrambling key and event information including payment amount corresponding to said associated event (Terms and Conditions page 4); and receives in said device, in response to user selection of said event, said digitally signed encrypted message (page 3 and page 6). The user device receives the program after requesting in program as shown on the figure on page 3. The system of Kaplan further authenticates, in the user, the source, the producer, of the digitally signed encrypted message in response to said digitally signed encrypted message (page 5 and page 7 Buying a Cryptolope part 2 and page 2 Cryptolope-a cryptographic envelope, paragraph 2); decrypting in said devices said digitally sired encrypted message to obtain said descrambling key upon said authenticating (page 7 Buying a Cryptolope part 5); receives, in said device, said selected event from the service provider (Publisher Content Creator paragraph), said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event (Figure on page 6); and descrambles, in said device, said selected event using said descrambling key (part 8 of Buying a Cryptolope page 7).

Although Kaplan discloses the authentication of the digital signature of the produces, the source, the system of Kaplan also discloses the authentication among participants. However Kaplan does not expressly disclose the authentication in the receiving device.

Renaud discloses a method, apparatus, and products are provided for verifying the authenticity of data within one or more data files (abstract). Renaud discloses the user receiving a signed file that it verifies the authenticity of the signed signature file (column 7 lines 48-62).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the contents of files as in Renaud using the digital signature and system of Kaplan. One of ordinary skill in the art would have been motivated to do this because digital signature verification provides a relatively high level of confidence in the authenticity of the source of the received data (Renaud column 2 lines 1-10).

Kaplan does not expressly disclose indicating the events that are available to the customer in the form of an electronic list of events.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to indicate the customer the types of events that are available in the form of a list of events. One of ordinary skill in the art would have been motivated to do this because a list is an organized and simple way of communicating information.

Although Kaplan discloses decrypting a digital signature during the authentication, Kaplan does not disclose using a first public key to obtain a second public key.

Schneier discloses Transfering keys using key-encryption keys to encrypt other keys for distribution (Page 176 Section 8.3 paragraph 3). Therefore decrypting the first key to obtain a second key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a key encryption key to encrypt another key as in Schneier to decrypt the digital signature of Kaplan. One of ordinary skill in the art would have been motivated to do this because key encryption key is a common method of distributing keys (Schneier page 176 section 8.3 paragraph 3).

In reference to claim 19, said device is a set-top box (page 1).

In reference to claim 20, the device is a digital television. The device suggested by Kaplan is a display device, a digital television is a display device (page 1).

Claims 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kaplan in view of Renaud and further in view of Vancelette.

In reference to claim 15, Kaplan discloses the cryptolope system wherein the user device receives an electronic list of events (programs; Figure on page 3), at least one event having a digitally signed encrypted message associated therewith (page 3), said encrypted message comprising a descrambling key and event information including payment amount corresponding to said associated event (Terms and Conditions page 4); and receives in said device, in response to user selection of said event, said digitally signed encrypted message (page 3 and page 6). The user device receives the program after requesting in program as shown on the figure on page 3. The system of Kaplan further authenticates, in the user, the source, the producer, of the digitally signed encrypted message in response to said digitally signed encrypted message (page 5 and page 7 Buying a Cryptolope part 2 and page 2 Cryptolope-a cryptographic envelope, paragraph 2); decrypting in said devices said digitally sired encrypted message to obtain said descrambling key upon said authenticating (page 7 Buying a Cryptolope part 5); receives, in said device, said selected event from the service provider (Publisher Content Creator paragraph), said selected event being scrambled using said descrambling key for preventing unauthorized access to said selected event (Figure on page 6); and descrambles, in said device, said selected event using said descrambling key (part 8 of Buying a Cryptolope page 7).

Although Kaplan discloses the authentication of the digital signature of the produces, the source, the system of Kaplan also discloses the authentication among participants. However Kaplan does not expressly disclose the authentication in the receiving device.

Renaud discloses a method, apparatus, and products are provided for verifying the authenticity of data within one or more data files (abstract). Renaud discloses the user receiving a signed file that it verifies the authenticity of the signed signature file (column 7 lines 48-62).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to authenticate the contents of files as in Renaud using the digital signature and system of Kaplan. One of ordinary skill in the art would have been motivated to do this because digital signature verification provides a relatively high level of confidence in the authenticity of the source of the received data (Renaud column 2 lines 1-10).

Kaplan does not expressly disclose indicating the events that are available to the customer in the form of an electronic list of events.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to indicate the customer the types of events that are available in the form of a list of events. One of ordinary skill in the art would have been motivated to do this because a list is an organized and simple way of communicating information.

Kaplan does not disclose the use of a smart card and descrambling performed in the smart card.

Vancelette discloses the steps of decrypting said message, receiving said selected event, and descrambling said selected event are performed in a smart card coupled to the device (column 9 lines 26-33). The message being encrypted using a public key associated with said

smart card and said step of decrypting uses a private key associated with and stored in said smart card, Vancelette suggests that this data is encrypted on the smart card since in the downloadable form the data is encrypted with the other data (column 6 lines 57-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize smart cards as disclosed in Vancelette in the system of Kaplan. One of ordinary skill in the art would have been motivated to do this because smart cards are small an efficient with increasingly more powerful processor.

In reference to claim 16 wherein said device is a set-top box (page 1).

In reference to claim 17 the device is a digital television. The device suggested by Kaplan is a display device, a digital television is a display device (page 1).

Claims 2-14, are rejected under 35 U.S.C. 103(a) as being unpatentable over the article by Kaplan and further in view of Renaud as in claim 1 and further in view of Vancelette.

In reference to claim 2, Kaplan does not disclose the use of a smart card and descrambling performed in the smart card.

Vancelette discloses the steps of decrypting said message, receiving said selected event, and descrambling said selected event are performed in a smart card coupled to the device (column 9 lines 26-33). The message being encrypted using a public key associated with said smart card and said step of decrypting uses a private key associated with and stored in said smart card, Vancelette suggests that this data is encrypted on the smart card since in the downloadable form the data is encrypted with the other data (column 6 lines 57-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize smart cards as disclosed in Vancelette in the system of Kaplan. One of ordinary skill in the art would have been motivated to do this because smart cards are small an efficient with increasingly more powerful processor.

In reference to claim 3, said message further comprises event information, said event information being decrypted using said private key (page 3).

In reference to claim 4, Vancelette discloses the event information is stored where the step is performed in the smart card (column 9 line 26-30). The information is downloaded to the terminals memory, the smart card has memory also and is situated at the terminal and is therefore available memory for the storage of the downloaded information.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize smart cards as disclosed in Vancelette in the system of Kaplan. One of ordinary skill in the art would have been motivated to do this because smart cards are small an efficient with increasingly more powerful processor.

In reference to claim 5, Vancelette discloses the smart card has a card body having a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 and PCMCIA card standards. It is inherent that the card body has terminals on its body for connection to the card reader for accessing the memory of the card.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize smart cards as disclosed in Vancelette in the system of Kaplan. One of ordinary skill in the art would have been motivated to do this because smart cards are small an efficient with increasingly more powerful processor.

In reference to claim 6, authenticating said list of events to verify the origin of said message. The events in the list are authenticated by the virtue of the list being encrypted by the service provider. The terminal then decrypts the packets with the corresponding key. This implies that only those with the key that corresponds the key of the service provider can decrypt the list and therefore the information comes from the service provider (page 2).

In reference to claim 8, event information comprises channel identification data, event identity data, date and time stamp data, and billing data (page 4).

In reference to claim 9, further comprising the step of storing said event information, wherein said step of storing said event information is performed in said device (page 6).

In reference to claims 13 and 14, said event information is used within said device to update said user's account information (column 2 lines 59-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the smart card as in Vancelette in the system of Kaplan. One of ordinary skill in the art would have been motivated to do this because smart cards are small and portable and have the processing power to perform encryption.

In reference to claims 7, Kaplan discloses the use of the private key used for digital signatures (page 3).

In reference to claim 10, Kaplan discloses digital signature, said second public key and said second private key are issued by an independent certificate authority and are associated with said list provider (page 6).

In reference to claim 11, said device is a digital television. The device suggested by Vancelette is a display device, 80, a digital television is a display device and is therefore the device suggested by Vancelette.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize smart cards as disclosed in Vancelette in the system of Kaplan. One of ordinary skill in the art would have been motivated to do this because smart cards are small an efficient with increasingly more powerful processor.

In reference to claims 12 said device is a set-top box (page 1).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Wednesday, December 13, 2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100